Blockchain and radio communications over suborbital spaceflights: Watchtowers and Mystics.

Sergio Martinez-Losa del Rincon*, Esteban Damian Gutierrez Mlot†
*Email: sergiomtzlosa@protonmail.com
†Email: esguti@protonmail.com

Abstract—**The communication between ground and satellites is tough due to long distances and interferences in the propagation medium. Using the blockchain technology and a serie of ground nodes, information can be distributed in a reliable and secure way. The satellite discovers nearby ground stations and send the information that it is verified with other nodes present in the same network. Ground nodes are classified in two types, master (Watchtowers) and working (Mystics) nodes. The Watchtower controls the entering gate of new nodes to the network and the distribution of information between the working nodes.**

The Mystics nodes use a verification process with the information. Each Mystic exchanges the information with the n-nearest nodes and receive tokens as a reward is the information has been verified using a proof-of-work algorithm.

Keywords-**Blockchain, high altitude satellite (hab), database, mystics, watchtower, distribution, network, realtime, proof-of-work, low-orbit, satellite.**

I. INTRODUCTION

Blockchain has been a disruptive technology in different fields. It is well known, the use of Blockchain in the cryptocurrencies [1], but there are other fields, like robotics [2], healthcare [3], software license validation [4] and more [5]. In our research process, we have not find any application in the field of the aeronautics, in particular suborbital devices, field whereby this paper presents the use of Blockchain and their advantages.

The main advantages of Blockchain are decentralization and immutability of the data. These two advantages perfectly fit with long flights communications like communications between a weather satellite and ground stations. The information in this kind of communications is transmitted primarily over the air and all over extensive areas. An extensive area of coverage needs on the ground a wide number of receptors collecting the information transmitted by the device. Blockchain creates a decentralized network of trusted nodes on the ground. The nodes can belong to different companies or even countries and thanks to blockchain, they can cooperate and trust each other, because the ledger of information shared cannot be stolen, corrupted or influenced by anyone.

In this paper, it is presented a novel method of Blockchain application in the fields of High Altitude Balloon (HAB) communications, that could be extended to other suborbital spaceflights communication. The method consist of maintaining a Blockchain Database (BDB) made up diverse nodes on land. The nodes synchronize the BDB when the HAB pass by their sphere of action. The BDB is filled with sensor data collected by the HAB. The consensus mechanism proposed for the participating ground nodes is the well-known Proof of Work (PoW). Although PoW has been used in our demonstration, we leave open the possibility of using other consensus mechanisms such as the novelty Proof of Stack (PoS) [6] or the much-studied Practical Byzantine Fault Tolerance (PBFT) [7].

The source code of the demostration is made available in a public repository [8].

II. BLOCKCHAIN AND LOW-ORBIT SATELLITES

In the dawn of the machines there was no communication over then, later on a set of protocols and different devices arise to interact between machine and humans.

The blockchain technology can be applied to low-orbit devices to send the data in a feasible and reasonable way. This technology ensures that data integrity is performed and also it can create a gratification token to users in order to maintain the network alive and make it grow.

The protocol described in this paper is based on two kinds of devices: the main device, hereinafter, the “Watchtower” and working nodes called “Mystics”.

A. Networking: Watchtower and Mystics

Every suborbital device belongs to one “Circle”. A Circle is the collection of devices and networks which receive, distribute and process the information related to one suborbital device.

Inside the Circle, the Watchtower is the gatekeeper. It has an active role in the network allowing or denying a node to be part of the Circle.

Not only nodes are controlled by the Watchtower, also information can be share between Circles through Watchtowers, making possible to communicate different suborbital devices in an isolated way.

Due to the high number of nodes that may become part of a Circle, it is allowed to have more than one Watchtower in the same network, avoiding bottlenecks.

A Mystic is in charge of processing and storing the information. Every Mystic must be registered on the

Watchtower before entering the Circle, that means Mystics must supply credentials to a Watchtower.

All Mystics are connected between them and with the Watchtower. A Mystic can belong only to one Circle but can switch to another Circle leaving the previous one.

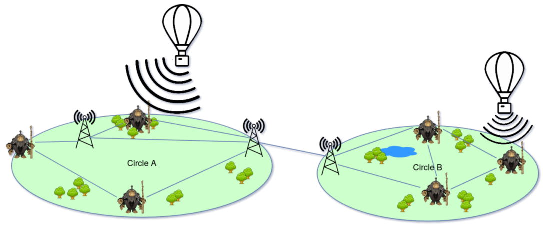

Figure 1. Mystics, Watchtowers and Circles.

B. Witchcraft and sorcery over data payload

This section will explain the process to obtain and distribute to all over the Circle from a particular Mystics.

Let's think that a suborbital device [9], [10] (for instance: low-orbit balloon) collecting data from several sensors and sending them thru an known (HTTPS) or unknow protocol to our Circle.

Each time the low-orbit satellite wants to send a new data, it sends a broadcast message to find Mystics and later on, from the returned response the satellite decides with one is the nearest from its current position. Once the low-orbit device selects the Mystic, it sends the data. Then, the data will be inside the Circle.

Each Mystic inserts the received data and get the hash resulting on the insertion in its blockchain. The Mystics send the calculated hash to the closest Watchtower. The Watchtower will order the hashes and select the most recent one. This hash will be sent it back to the Mystics which gave hashes to the Watchtower.

Each Mystic updates its own stored data by talking and exchanging information with the n-nearest Mystics in a data verification process, thus all Mystics have the same information. On this verification process each Mystic receives a gratification token called "Sparkling". There is a delay time of 15 minutes between each Mystic-to-Mystic update. The data will be considered as verified when the 80% of the circle or more verify the data.

As additional security operation, after data verification, the Watchtower ask to n-random number of Mystics for their last hash, if the hashes between the Watchtower and the Mystics match, the Mystics have been updated accurately.

This process can be repeated on each circle, it is important to know that the satellites can only discover one or more circles if the satellite has the Circle identification, this identification must be a long, unique and hexadecimal token generated on ground before landing.

There are more ways to identify a remote device against a Circle, the proposed way is one of them but there are many others like name and password, two-factor authentication, asymmetric cryptography [11], or LDAP server. The method proposed in this paper has been selected because is the simplest way to authenticate consuming the lowest power possible.

The Circle token cannot be shared and it is generated per satellite and flight. It is mandatory that the identification has been on board when the low-orbit device leaves ground, because it will not be possible to update it during the flight.

C. Data update between Mystics

All Mystics are connected in the same circle. A Mystic sends the last data available on its blockchain to the n-nearest Mystics. After the insertion of data, the Mystics match the token. If the tokens are equal, then the data is verified. This process is repeated on each Mystic until reach the 80% (or more) of the available Mystics on the circle.

If the data cannot be verified by the Mystics,the data insertion is revoked and information discarded.

D. Communication between Watchtowers of different circles

The Watchtowers are the gateway between circles. They exchange trust tokens that allow external Mystics to login into another circle, these tokens can be revoked at any time.

The token is build with an exchange of credentials between the Watchtowers. Let's explain the token exchange with an example:

1) Watchtower A (WA) wants to enter into circle B (CirB) lead by Watchtower B (WB).
2) WA sends a request to WB and WB responds with a token revocable after 15 min.
3) if WA wants more than 15 minutes, it will perform a second request using the current temporal token and requesting a time window for n-minutes.
4) If the 15 minutes token expires the WA can request another 15 token to WB.

E. Black Mystics: Sorcery forks

It is not intended to have fork on the circle as the information only enter using only one Mystic. It is a future tasks to know how behaves the circle over sorcery forks.

F. Mystics lifecycle: crossing the life abyss

The Watchtower sends discovering packets (charm) every n-minutes to know if all registered Mystics are alive.

Once the lifecycle of a Mystic is over and it crosses the life abyss, the Mystic stops making sorcery at the circle and the Watchtower removes the Mystics from the alive Mystics list [1] to the abyss list. A Mystic can back again to the Circle performing again a registering request. The Watchtower has the information of the dead-and-gone Mystics and can return them back to life in the circle.

---

[1] [illegible]

G. *Circle security enhancement*

It is not implemented yet a method to avoid the 51% attack [12]–[14] over the network. This circumstance sets the limit of external Mystics from a foreign circle in (n/2)-2 where n-item is the number of Mystics from our circle. This limit adds up 2 foreign Mystics to our circle, 2 instead of 1 to avert fails. It is a future task to find a better system to avoid this kind of attacks.

III. DEMO FOR A PROOF OF CONCEPT

This demo shows the proposed system as a proof of concept. Although the system needs dozens of Mystics on ground and at Watchtower to show the true potential of this idea, we are going to show a low-scale infrastructure just for demonstration purposes.

The demonstration consists in a Circle with 3 Mystics and a Watchtower. The Circle is isolated from other circles and obtains the data from a external source (for instance, a weather balloon which is a low-orbit device).

We have uploaded the source code to a public repository [8]. Have in mind that the code is in continous development and could be incomplete.

A. *Hardware proposed*

The hardware list for this proof of concept is the following:

- 3 Raspberry Pi 3B+ to work as Mystics
- 1 Raspberry Pi 3B+ to work as Watchtower
- Ethernet cable Cat6
- Router with internet access
- A low-orbit device with sensors

B. *Software proposed*

The low-level system to store the data is a non-relational database because this kind of databases has good performance with blockchain technology [15], [16]. In particular, in this demo we will use MongoDB [17] as it easy to use and it fits our needs.

As communication protocol between the external source (satellite) and the Circle, we choose HTTPS, because it is a lightweight and well-know communications protocol.

It is also necessary a set of Web Services to send the information to the circle, then it is used PHP as programming language to build these services. The service will be onto an Apache2 server

The payload to send is not define by now but we will use JSON [18] notation to create a payload structure.

The security related to external nodes, is build-in with a time-token system. This token is used by external Mystics which want to enter to the circle. There is also a firewall to avoid DoS attacks [19], [20], just necessary to open a port for the Web Services.

C. *Demo explanation and results*

The objective of this demo is to know how behaves a home made blockchain network with time-tokens security.

On this circle all Mystics are connected between them and each Mystic is connected to the Watchtower.

The demo performed well accurately and the results were what we expected. The only issue found, was that the time verification of the data inserted in the blockchain is quite high (around 5 seconds). This issue is due to the low-powered hardware used in the demo.

The data were secure and the Watchtower perform well within this infrastructure.

IV. CONCLUSION AND FUTURE WORK

The system has to be tested with a bigger circle with more Mystics and Watchtowers interacting between them. A bigger circle will let us achieve more accurate results.

The demo proposed is low-scaled, and maybe the results will be different in a larger network. The non-relational database gives little delay with few nodes on the network, it is a future work to find a better solution or try with other non-relational database with better performance.

The WebServices performed well and we cannot measure high delays on communications over low-orbit devices, in the future we will study a replacement to Web Services as alternative communication technology.

In conclusion, the communications between satellites and ground station can be faster and near real time with blockchain technology, it is in our hands to develop a new way to obtain a big amount of data from the current system. A bigger set of data will set us into a new edge of possibilities and challenges regarding the keep and distribution of the data.

REFERENCES

[1] Satoshi Nakamoto et al., "Bitcoin: a peer-to-peer electronic cash system," 2008.

[2] A. Mushtaq and I. U. Haq, "Implications of blockchain in industry 4.o," in *Proc. Int. Conf. Engineering and Emerging Technologies (ICEET)*, Feb. 2019, pp. 1–5.

[3] T. Abdullah and A. Jones, "ehealth: Challenges far integrating blockchain within healthcare," in *Proc. Safety and Sustainability (ICGS3) 2019 IEEE 12th Int. Conf. Global Security*, Jan. 2019, pp. 1–9.

[4] S. Bayhan, A. Zubow, and A. Wolisz, "Spass: Spectrum sensing as a service via smart contracts," in *Proc. IEEE Int. Symp. Dynamic Spectrum Access Networks (DySPAN)*, Oct. 2018, pp. 1–10.

[5] M. AbuNaser and A. A. Alkhatib, "Advanced survey of blockchain for the internet of things smart home," in *Proc. IEEE Jordan Int. Joint Conf. Electrical Engineering and Information Technology (JEEIT)*, Apr. 2019, pp. 58–62.

[6] Anjani Barhanpure, Paaras Belandor, and Bhaskarjyoti Das, “Proof of stack consensus for blockchain networks,” in *SSCC*, Sabu M. Thampi, Sanjay Madria, Guojun Wang, Danda B. Rawat, and Jose M. Alcaraz Calero, Eds. 2018, vol. 969 of *Communications in Computer and Information Science*, pp. 104–116, Springer.

[7] Miguel Castro and Barbara Liskov, “Practical byzantine fault tolerance,” Berkeley, CA, Feb. 22–25 1999, pp. 173–186, Usenix Association.

[8] Sergio M-L.R. and Esteban D.G.M, “blockchain-satellite,” https://github.com/sergiomtzlosa/blockchain-satellite, 2019.

[9] J. Andrusenko, J. L. Burbank, and W. T. Kasch, “Augmentation of military satellites with high altitude balloons: A UHF case study,” in *Proc. IEEE Aerospace Conf*, Mar. 2005, pp. 1–16.

[10] T. H. Dinh, D. Niyato, and N. T. Hung, “Optimal energy allocation policy for wireless networks in the sky,” in *Proc. IEEE Int. Conf. Communications (ICC)*, June 2015, pp. 3204–3209.

[11] Rotraut Laun, “Asymmetric user authentication,” *Computers & Security*, vol. 11, no. 2, pp. 173–183, 1992.

[12] C. Natoli and V. Gramoli, “The blockchain anomaly,” in *Proc. IEEE 15th Int. Symp. Network Computing and Applications (NCA)*, Oct. 2016, pp. 310–317.

[13] T. P. Keenan, “Alice in blockchains: Surprising security pitfalls in pow and pos blockchain systems,” in *Proc. Security and Trust (PST) 2017 15th Annual Conf. Privacy*, Aug. 2017, pp. 400–4002.

[14] J. Bae and H. Lim, “Random mining group selection to prevent 51% attacks on bitcoin,” in *Proc. 48th Annual IEEE/IFIP Int. Conf. Dependable Systems and Networks Workshops (DSN-W)*, June 2018, pp. 81–82.

[15] Elena Karafiloski and Anastas Mishev, “Blockchain solutions for big data challenges: A literature review,” in *IEEE EUROCON 2017-17th International Conference on Smart Technologies*. IEEE, 2017, pp. 763–768.

[16] Victoria L Lemieux, “A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation,” in *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, 2017, pp. 2271–2278.

[17] Inc. MongoDB, “mongoDB,” https://www.mongodb.com/, 2019, [Online; accessed 03-Oct-2019].

[18] Charles R. Severance, “Discovering javascript object notation,” *IEEE Computer*, vol. 45, no. 4, pp. 6–8, 2012.

[19] B. T. Asare, K. QuistâĂŞAphetsi, and L. Nana, “Nodal authentication of iot data using blockchain,” in *Proc. Computational Modelling and Applications (ICCMA) 2019 Int. Conf. Computing*, Mar. 2019, pp. 125–1254.

[20] F. Alkurdi, I. Elgendi, K. S. Munasinghe, D. Sharma, and A. Jamalipour, “Blockchain in iot security: A survey,” in *Proc. 28th Int. Telecommunication Networks and Applications Conf. (ITNAC)*, Nov. 2018, pp. 1–4.